

REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 and 22-26 are pending in the present application. No claim amendments are presented, thus no new matter is added.

In the Office Action, Claims 22-25 are rejected under 35 U.S.C. § 112, first paragraph; Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 and 26 are rejected under 35 U.S.C. § 103(a) as unpatentable over Timmer (U.S. Pub. 2002/0107895) in view of Shurts (U.S. Pat. 5,572,673); and Claims 22-25 are rejected under 35 U.S.C. § 103(a) as unpatentable over Timmer in view of Shurts and An et al. (U.S. Pub. 2002/0077062, herein An).

The Office Action rejects Claims 22-25 under 35 U.S.C. § 112, first paragraph, asserting that the feature of “passively receiving metadata transmitted from a device located at an entrance of a facility” is not described in the specification. Applicant respectfully traverses this rejection.

With respect to the written description requirement, there is no *in haec verba* requirement, and claim limitations may be supported by the specification through ***express, implicit, or inherent*** disclosure.¹ To satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention.²

If a skilled artisan would have understood the inventor to be in possession of the claimed invention at the time of filing, even if every nuance of the claims is not explicitly described in the specification, then the adequate description requirement is met. See, e.g., *Vas-Cath*, 935 F.2d at 1563, 19 USPQ2d at 1116; *Martin v. Johnson*, 454 F.2d 746, 751, 172

¹ MPEP § 2163.

² *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555 (Fed. Cir. 1991).

USPQ 391, 395 (CCPA 1972) (*stating "the description need not be in *ipsis verbis* [i.e., "in the same words"] to be sufficient"*).

Thus, the failure to use the express term "passively" in the specification is an insufficient basis for concluding lack of written description, since at least p. 21, ll. 10 – 18 of the specification describes how data may be transmitted to a device by merely passing through an entrance of a location that transmits the metadata (i.e. passively).

The analysis of whether the specification complies with the written description "is conducted from the standpoint of one of skill in the art. Generally, there is an inverse correlation between the level of skill and knowledge in the art and the specificity of disclosure necessary to satisfy the written description requirement."³

Moreover, the MPEP discusses several factors that must be considered in order to make a 112, first paragraph, rejection for lack of written description. The MPEP states:

Whether the specification shows that applicant was in possession of the claimed invention is not a single, simple determination, but rather is a factual determination reached by considering a number of factors. Factors to be considered in determining whether there is sufficient evidence of possession include the level of skill and knowledge in the art, partial structure, physical and/or chemical properties, functional characteristics alone or coupled with a known or disclosed correlation between structure and function, and the method of making the claimed invention.

* * * *

The description needed to satisfy the requirements of 35 U.S.C. 112 "varies with the nature and scope of the invention at issue, and with the scientific and technologic knowledge already in existence." *Capon v. Eshhar*, 418 F.3d at 1357, 76 USPQ2d at 1084.

* * * *

Thus, an inventor is not required to describe every detail of his invention. An applicant's disclosure obligation varies according to the art to which the invention pertains. Disclosing a microprocessor capable of performing certain functions is sufficient to satisfy the requirement of section 112, first paragraph, when one skilled in the relevant art would understand what is intended and know how to carry it out."⁴

³ Page A-7 of the USPTO's *Written Description Training Materials*, revision 1, March 25, 2008.

⁴ MPEP §2163, emphasis added.

The outstanding Office Action fails to provide any explicit analysis as to the above-noted factors, which are pertinent to a determination of compliance with the written description requirement. Thus, the outstanding Office Action has failed to set forth a *prima facie* case of failing to comply with the written description requirement.

Further, at least p. 21, ll. 10 – 18 of the specification describes seamlessly interacting with wireless environments regardless of the location of the user. Examples of such environments include restaurants, movie theaters, and bowling alleys. A transmitter is installed at the entrances to these facilities without exception. That is, an infrastructure for writing data as users' history information (history data) is built, and when a user enters a movie theater, such information as "16:00, April 15, Titanic" is inputted to the information communication device 1 carried by the user. Thus, this metadata is passively (i.e. without action by the user) transmitted from a device located at an entrance of a facility.

Thus, a person of ordinary skill in the art would recognize that the inventor was in possession of the claimed invention at the time of filing and the written description requirement is satisfied. The rejection under 35 U.S.C. §112, first paragraph, should be withdrawn.

The Office Action rejects independent Claims 1, 7, 13, 16, 19 and 20 under 35 U.S.C. § 103(a) as unpatentable over Timmer in view of Shurts. Applicant respectfully traverses this rejection as independent Claims 1, 7, 13, 16, 19 and 20 recite novel features clearly not taught or rendered obvious by the applied references.

Independent Claim 1, for example, recites a mobile information communication device, comprising:

... a central control unit which ...stores metadata received through said wireless communication unit in a corresponding partition of the metadata storage unit based on matching the received metadata with a security level and/or category predetermined by the user, and ***sets a higher security level for***

data received through a relatively secure communication path and a lower security level for other received data...

Independent Claims 7, and 19, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of independent Claims 1, 7 and 19.

In rebutting the previously presented arguments directed to the above emphasized claimed feature, p. 3 of the Office Action asserts that Timmer “does teach distinguishing the type of network used to exchange data between a client and a host as having different security levels.” Applicant respectfully traverses this assertion.

Particularly, p. 3 of Office Action cites paragraph [0088] of the publication of the present application that describes, in an exemplary embodiment, that telephone and e-mail communications are assigned a higher security level than other transmitted data. More particularly, as shown in an exemplary embodiment at Fig. 5 of the disclosure, the security level of received data is *set* to be higher for data received via a relatively secure communication path (e.g., transmissions and conversations by telephone, electronic or the like), versus other received data (e.g., metadata received from local wireless transmitters). In other words, as described in an exemplary embodiment at paragraphs [0089] – [0100] of the specification, conversations over e-mail or using the telephone function may be assigned a higher security level than communications performed via short range wireless communications (e.g., UWB) with a device that transmits metadata regarding a television show a user is watching or a location into which the user has entered.

The Office Action then cites paragraph [0010] of Timmer, and asserts that since this cited portion of the reference receives different types of messages, that this features reads on the claimed feature of “***setting a higher security level for data received through a relatively secure communication path and a lower security level for other received data***”. Timmer,

however, fails to remotely teach or suggest that the different types of received data are received “*through a relatively secure communication path*” versus “*other received data*”, whatsoever, much less “*setting a higher security level for data received through a relatively secure communication path and a lower security level for other received data*”, as claimed. Moreover, the Office Action fails to cite any portion of Timmer as even suggesting that the different types of received data are received “*through a relatively secure communication path*” versus “*other received data*”, as claimed.

As noted above, the Office Action appears to rely on the description that Timmer can receive various types of data, as meaning that these types of data are handled as having differing security levels. Timmer, however, fails to teach or suggest any such feature.

Regarding Shurts, col. 1, l. 53 – col. 2, l. 5 of this reference describes that a security policy, known as "mandatory access control" or MAC, gives "subjects" access to database objects on the basis of sensitivity labels only. A subject is an active entity, such as a user at a workstation or a command that acts on behalf of the user. An object is a passive entity that contains or receives information. Examples of objects include database tables, rows, views, and procedures. Before any object is accessed in a MAC system, the subject's sensitivity label is compared with the object's sensitivity label to determine whether the subject is allowed to access the object in the manner requested.

Thus, the cited portion of Shurts merely describes that a subject's sensitivity level is compared against a sensitivity level of an object being accessed in order to determine whether the subject may have a label that dominates the object. Moreover, Shurts, at col. 7, ll. 24-41, for example, describes that a change in the security level of an object requires an evaluation of the object by a security officer (SSO) and an initiated internal database procedure to change the status of the object. Therefore, if the system of Shurts were modified to assign security levels of the objects based on a path on which the object was received, it would

render the system unfit for its intended purpose by taking the task of changing/assigning the security settings out of the hands of the SSO.

Therefore, Shurts and Timmer, neither alone, nor in combination, teach or suggest a mobile information communication device that includes “a central control unit which ... ***sets a higher security level for data received through a relatively secure communication path and a lower security level for other received data...***,” as recited in amended independent Claim 1.

Accordingly, Applicant respectfully request that the rejection of Claim 1 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 7 and 19 also patentably define over Timmer and Shurts.

Regarding independent Claims 13, 16 and 20, Claim 13, for example, recites an information exchange and human relation fostering support system for supporting information exchange and fostering of human relations between a plurality of users in the virtual world, comprising:

...at least one stationary communication device configured to acquire metadata from each mobile information communication device via a wireless transmission, ***compare the acquired metadata and display the result of the comparison.***

In rebutting the previously presented arguments regarding the above emphasized claimed feature, p. 5 of the Office Action cites Claim 1 and seems to assert that the feature of “supplies, in response to an external access request, metadata from the metadata storage unit that matches a security level available to the external access request” is analogous to the “compare” feature recited in independent Claim 13. Particularly, the Office Action asserts that “claim 1 shows that the supplied data is the data that matches the security level available to the requestor. This inherently requires a comparing and determining whether the security level of data matches that of the requestor.”

However, it is difficult to determine how “supplying ... metadata from the metadata storage unit that matches a security level available to the external access request” is considered to be the same limitation as “at least one stationary communication device configured to acquire metadata from each mobile information communication device via a wireless transmission, *compare the acquired metadata and display the result of the comparison.*” At best, the limitation in Claim 1 requires that the communication device compare an access level of a received request to an access level of metadata stored in the communication device, but does not read on “at least one stationary communication device configured to *acquire metadata from each mobile information communication device via a wireless transmission* [and] *compare the acquired metadata and display the result of the comparison,*” as recited in Claim 13. More particularly, comparing a security level of a received request to a security level of stored metadata is not the same as *comparing metadata acquired from each mobile information communication device*, as claimed.

Moreover, the Office Action notes that “Applicant’s arguments completely ignores the basis of rejection ...” However, Applicant notes that there still exists no basis for the rejection of the above noted claimed feature recited in Claim 13. As noted above, the features of Claim 13 are not the same as those recited in Claim 1, and should not be rejected as being “substantially the same”, as noted at p. 13 of the Office Action.

The Office Action, therefore, again fails to address the above noted claim feature, and Applicant respectfully submits that Timmer and Shurts, neither alone, nor in combination, teach or suggest a stationary communication device the acquires and compared metadata, as required by independent Claims 13, 16 and 20.

Moreover, independent Claims 16 and 20 recite the additional features of:

... comparing the uploaded metadata to find matching activities and interests;

***displaying the matching activities and interests and corresponding users discovered by the comparing;
deleting the uploaded metadata from the stationary communications device.***

In citing a new portion of Timmer to reject the claimed “comparing” feature, p. 5 of the Office Action relies on paragraph [0031] of this reference, apparently asserting that the process of downloading and sharing reviews of restaurants “must be able to compare data to find matching activities and interests”. The Office Action, however, fails to provide any reasonable basis why a user’s scrapbook application, in which they may publish reviews of restaurants, must be able to compare data to find matching activities an interests. More particularly, the entire purpose of Timmer is to allow a user to publish a scrapbook that can be accessed by other users via the Internet, and these users may browse the published scrapbook. Thus, there exists no mechanism by which the scrapbook must be able to compare data to find matching activities an interests because the scrapbook does not receive metadata from users for purposes of comparison. More particularly, someone who access the scrapbook in Timmer merely browses the scrapbook, and does not ***upload metadata*** for comparison, as claimed.

In rejecting the feature directed to “***displaying the matching activities and interests and corresponding users discovered by the comparing***”, the Office Action cites paragraph [0031] of Timmer, which describes that a scrapbook may be made to travelers who are taking similar trips. As noted above, however, this cited portion of Timmer merely describes a process of publishing a scrapbook of a trip taken by the author, and fails to teach or suggest comparing metadata of users whatsoever. Instead, Timmer merely describes that the scrapbook may be “made available and shared according to the user’s choice ...” Timmer, therefore, fails to teach or suggest that this “displaying” is performed as a result of any comparing of received metadata, as recited in Claims 16 and 20.

Therefore, Timmer fails to teach or suggest at least the features of “*comparing the uploaded metadata to find matching activities and interests*” and “*displaying the matching activities and interests and corresponding users discovered by the comparing*”, as recited in independent Claims 16 and 20.

Accordingly, for at least the reasons discussed above, Applicant respectfully requests that the rejection of Claims 13, 16 and 20 (and any claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn.

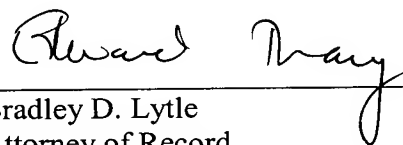
Regarding the rejection of Claims 22-25 under 35 U.S.C. § 103(a) as unpatentable over Timmer in view of Shurts and An, Applicant notes that Claims 22-25 depend from one of independent Claims 1, 7, 13 and 19, and are believed to be patentable for at least the reasons discussed above. Moreover, Applicant respectfully submits that An fails to remedy the above noted deficiencies of Timmer and Shurts.

Accordingly, Applicant respectfully requests that the rejection of Claims 22-25 under 35 U.S.C. § 103 be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3, 5-7, 9, 11-13, 15, 16, 18-20 and 22-26 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

A handwritten signature in cursive script, appearing to read "Bradley D. Lytle", is written over a horizontal line.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Andrew T. Harry
Registration No. 56,959